The S Unit Offensive Security

DE SECURITY UPDATE

Kan ChatGPT pentesten uitvoeren?

Cees Duivenvoorde
CEO The S-Unit
cduivenvoorde@the-s-unit.nl

In een recente publicatie stelt onderzoeksinstituut TNO dat “banken en andere cruciale Nederlandse bedrijven zo snel mogelijk hun cyberveiligheid volledig uit handen moeten geven aan kunstmatige intelligentie (AI)”

Oei, een bedreiging voor onze business?

De razendsnelle evolutie van AI dit jaar is niemand ontgaan. De consequenties voor de maatschappij zijn echter nog onduidelijk. Er wordt hevig over gespeculeerd en de meningen zijn verdeeld. AI in 2014 zei natuurkundige Stephen Hawking over AI: ‘De ontwikkeling van kunstmatige intelligentie kan het einde van de mensheid betekenen.’ en ‘De mens kan die groei niet bijhouden, omdat biologische evolutie hen tegenhoudt. De mens wordt dan voorbijgestreefd.’ Moeten we ons zorgen maken, of is het juist een goede ontwikkeling en hoe houden we het onder controle?

Een Large Language Model zoals ChatGPT is in staat grote hoeveelheden data te verwerken en de daarin opgesloten kennis te gebruiken. ChatGPT combineert informatie en reproduceert kennis op basis van de data waarmee het is getraind. Maar ‘begrijpt’ ChatGPT ook echt de onderliggende data en verbanden, zodat het nieuwe inzichten krijgt? En in hoeverre zijn eventuele nieuwe inzichten van belang om de cyberveiligheid te waarborgen? Hier raken we het verschil tussen Defensive Security en Offensive Security.

Defensive Security

Het advies van TNO gaat met name over XDR (Extended Detection and Response), de defensieve kant van cyberveiligheid. Het snel herkennen van een aanval en het snel reageren is cruciaal en bij uitstek iets wat AI goed kan. Als AI getraind is met goede data (zie de consultancy blog op pag. 4) dan wordt een aanval snel gedetecteerd en kan er ook direct goed gereageerd worden. Het doorlopend blijven trainen op basis van nieuwe actuele data is hierbij ook cruciaal. En een effectieve XDR werkt alleen bij herkenning van nagenoeg alle dreigingen. Op dit vlak is de tweede voorspelling van Hawking al uitgekomen. De mens is niet in staat om de enorm snel groeiende hoeveelheid security data die beschikbaar komt bij te houden en AI wel. Het gaat om weten wat de actuele dreigingen zijn en die kennis direct toepassen. AI is ons voorbijgestreefd.

Offensive Security

En dat is ook direct het verschil met Offensive Security. Natuurlijk bestaat het zoeken naar kwetsbaarheden voor een deel ook uit het inventariseren van bekende kwetsbaarheden: het deel van het pentest proces dat mogelijk te automatiseren is. Maar een belangrijk deel van offensive security is ook het zoeken naar nieuwe kwetsbaarheden of het zoeken naar nieuwe geavanceerde mogelijkheden om (combinaties van) kwetsbaarheden te exploiteren. En dan is het niet alleen van belang kennis te hebben van security en kwetsbaarheid en, maar ook en vooral om deze te begrijpen. Zodat op basis van inzicht, i.p.v. louter kennis, nieuwe kwetsbaarheden ontdekt kunnen worden, of misschien beter gezegd: uitgevonden kunnen worden. En dat is bij uitstek waar de mens met ‘echte’ intelligentie excelleert boven de ‘kunstmatige’ intelligentie van systemen als ChatGPT.

Dit is ook het vlak van security waar The S-Unit zich al 10 jaar in probeert te onderscheiden. Wij gebruiken geautomatiseerde tooling om kennis te vergaren over het te testen systeem (bijvoorbeeld infra, webportal, API of softwareplatform), om het systeem te leren begrijpen. En ons begrip van het te testen systeem leidt tot nieuwe inzichten en op basis daarvan vinden we kwetsbaarheden die niet gevonden worden met geautomatiseerde tooling, en naar ons inzicht voorlopig ook nog niet door AI.

Samenvattend: In cybersecurity moet je weten hoe je kunt verdedigen en moet je begrijpen hoe je kunt aanvallen. Terwijl AI een rol kan en gaat spelen in de verdediging, blijft menselijk begrip en inzicht onvervangbaar in de kunst van het aanvallen.

RUBRIEKEN

Volg ons ook op LinkedIn

CYBERCRISIS SIMULATIE

Is jouw organisatie voorbereid op een cybercrisis? Test de weerbaarheid van jouw organisatie tijdens een realistische cybercrisis simulatie van The S-Unit!

RED TEAMING

De kern van offensieve security ligt in het bekijken van security door de bril van een hacker. Dichterbij deze blik kun je niet komen dan met een red teaming. Middels een realistische aanvalssimulatie meten wij de weerbaarheid van jouw organisatie tegen een aanvaller. Waar een penetratietest gezien kan worden als een proefwerk, is een red teaming het eindexamen.

PENTESTEN

Offensive security begint vaak met een penetratietest. Want we snappen dat je wilt weten óf en waar jouw organisatie kwetsbaar is. Daarbij kijken we natuurlijk naar wat voor jou belangrijk is. De kroonjuwelen. Het is de missie van onze hackers om inzicht te krijgen in de beveiligingsstatus van jouw IT. En dat vervolgens te vertalen naar heldere inzichten en concrete verbeterpunten.

TRENDS, NIEUWS & INZICHT

Met een proactieve houding houden de security experts van The S-Unit de belangrijkste bronnen strak voor jou in de gaten om je te voorzien van de belangrijkste en meest actuele dreigingen die op jouw organisatie van toepassing zijn.

AI gevaarlijk! Maar waarom eigenlijk?

Met de brede publieke beschikbaarheid van Artificial Intelligence (AI), of eigenlijk Large Language Model (LLM), lijken we technologieën binnen handbereik te hebben waarvan in de media wordt gezegd dat deze óf onze ondergang worden óf al onze wereldproblemen gaan oplossen. Duidelijk is het dat het iets is dat ons kan helpen. Zowel de goede als de kwade. Iets kan altijd op oneigenlijke wijze worden ingezet. Bewust of onbewust. Door verschillende media wordt aangehaald dat cybercriminelen nog gevaarlijker worden vanwege de mogelijkheden van LLM. Maar wat zijn deze gevaren eigenlijk? Welke risico's brengt het publiekelijk beschikbaar maken van Artificial Intelligence met zich mee? Wat zijn de offensieve gevaren van AI? In dit artikel beschrijven wij een aantal van deze offensieve gevaren van Artificial Intelligence.

Een inmiddels bekend risico heeft betrekking op de gevolgen van gegevenslekken door de AI-systemen. Door het lerende vermogen wordt hetgeen in de LLM wordt gestopt opnieuw gebruikt in vervolg vragen. In een eenvoudig voorbeeld waarbij programmacode wordt geschreven met behulp van AI, en hierin autorisatiesleutels worden geknipt en geplakt, zijn deze sleutels 'beschikbaar' in een andere niet gecontroleerde omgeving. Het is mogelijk dat deze sleutels publiekelijk toegankelijk worden en in een volgende AI-chat worden weergegeven. Een aanvaller hoeft enkel actief op zoek te gaan naar sleutels vanuit de vraag aan de AI-chat voor ondersteuning in het schrijven van code die de authenticatie uitvoert op basis van autorisatiesleutels binnen een programma. De kans bestaat dat voorbeelden worden gegeven van code die autorisatiesleutels bevat. Daarna moet van deze sleutels ook nog worden gevalideerd of deze daadwerkelijk misbruikt kunnen worden. Hierin zit, in eerste instantie, nog een groot deel handwerk en uitvraag werk.

Binnen de informatiebeveiliging is AI als onderdeel van beveiligingssystemen niet meer weg te denken. Met behulp van AI-systemen is het mogelijk om heel snel te leren van en over afwijkende patronen om zo beoordelingen uit te voeren om personen of programma's te blokkeren dan wel door te laten. Juist dit lerende vermogen op basis van een hoeveelheid trainingsdata is ook gelijk de zwakte van deze systemen, waar een aanvaller misbruik van kan maken. Door de AI-modellen te manipuleren met misleidende gegevens worden verkeerde beslissingen genomen. De inbraakdetectiesystemen of malware-detectoren falen; medewerkers worden geblokkeerd, de aanvallers worden doorgelaten en malafide software wordt geïnstalleerd. Deze autonome beslissingen kennen ook het gevaar dat de mens geen controle meer heeft.

Daarnaast kan het verwerken van grote hoeveelheden gegevens en het uitvoeren van repetitieve taken door AI-systemen ook als aanval worden ingezet. Bijvoorbeeld het zonder grote inspanning versturen van massale desinformatie via sociale media of het eindeloos uitvoeren van phishing-aanvallen. Maar ook het moeiteloos uitvoeren van doorlopende 'controles' van kwetsbaarheden op publiekelijk beschikbare systemen. Met de toegevoegde intelligentie wordt gepoogd de kwetsbaarheden ook daadwerkelijk uit te buiten. Dus los van inzicht in kwetsbaarheden is ook het inzicht in te misbruiken kwetsbaarheden beschikbaar.

Ondanks dat dit al geruime tijd wordt toegepast, is vooral de schaalbaarheid van en toegankelijkheid tot deze informatie een realistisch gevaar. Voor een grotere groep 'kwaadwillende' is informatie over kwetsbare systemen beschikbaar. Tel hierbij op de ondersteuning van AI-chats bij het helpen bouwen van kwaadwillende software om kwetsbaarheden te misbruiken, iets wat voorheen enkel door een beperkte groep werd uitgevoerd, en een ongekend groot leger is in staat om aanvallen uit te voeren. Waarvan een deel mogelijk niet eens het besef heeft van wat zij daadwerkelijk aan het doen zijn. Met als toevoeging dat de huidige AI's nog niet zo goed zijn dat ze perfecte code schrijven.

Het lerende vermogen en het eindeloos geduldig uitvoeren van taken maken AI-systemen zeer geschikt voor het uitvoeren van phishing-campagnes en social engineering. Sinds de publieke lancering van ChatGPT zijn de phishingmails 'beter' geworden, aldus verschillende onderzoeken. De mails zijn minder algemeen, specifieker op maat en zeer moeilijk van echt te onderscheiden. De standaard berichten van weleer worden automatisch voorzien van de specifieke bedrijfsgegevens.

Door het lerende vermogen worden gemakkelijk zogenaamde deepfakes geproduceerd, om in audio of videovorm de gebruikers te misleiden. Waar in het verleden een berichtje vanuit de naam de van directeur een bekende manier was om vertrouwen te krijgen en (niet) te reageren, is het nu mogelijk een telefoontje of voicemail – met de stem – van de directeur te sturen om dit vertrouwen te krijgen.

Als laatste is er nog het hallucinerende vermogen. Niet direct een offensief probleem, maar wel lastig als je op basis van een door AI gegenereerd boek paddenstoelen gaat zoeken. In het boek, dat als e-book werd aangeboden via een grote bekende webshop, werd het proeven aangeraden als methode om gevaarlijke en onschuldige paddenstoelen van elkaar te onderscheiden. Hoe kan je redelijkerwijze nog vertrouwen welke informatie juist is?

Zoveel dreigingen! Hoe te beschermen?
De bovengenoemde risico's zijn in beginsel niet geheel nieuw, maar de uitvoering is in een nieuw jasje gestoken. Reeds aanwezige bescherming kan in veel situaties volstaan, maar aanvullende en 'meegroeiende' maatregelen zijn wenselijk.

De belangrijkste factoren zijn de snelheid waarmee de aanvallen worden uitgevoerd en de frequentie waarmee het type aanval verandert. De mitigerende maatregelen vereisen dan ook aandacht vanuit deze factoren. Bijvoorbeeld door medewerkers vaker op de hoogte te brengen van de ontwikkelingen van mogelijke aanvallen. Dus vier keer per jaar een phishingcampagne in plaats van jaarlijks. Vaker korte berichten over de manier waarop zij kunnen helpen de omgeving veilig te houden. Maar ook het bijbrengen van wat wel en niet kan of gewenst is met behulp van AI binnen de organisatie.

Kwetsbaarheden in systemen dienen zo snel als mogelijk verholpen te worden, vrijwel gelijk met het uitkomen van de patches. Inzicht in de kwetsbaarheden kan verkregen worden door penetratietesten. Het afwisselen van deze testen met andere vormen van testen, zoals Red Team-testen, geven een nog beter beeld in het geheel van schakels in de securityorganisatie.

Audit trails en logboeken verdienen ook aanvullende aandacht. Gebruik hierbij een SIEM oplossing, waarbij deze specifieker is geconfigureerd dan de standaardregels. Blijf de uitkomsten van de oplossing volgen en bijstellen. Dit is een onderdeel van het continu monitoren en bijstellen; blijf gevoel houden welke activiteiten plaats vinden in de omgeving. Blijf op de hoogte van de ontwikkelingen van aanvalstechnieken zodat de beveiligingsmaatregelen hierop aangescherpt kunnen worden.

Blijf nieuwsgierig, blijf ontwikkelen!

Bas Labordus - Security Consultant The S-Unit

Ray van Daalen

Als operationeel manager ontfermt Ray zich over het reilen en zeilen binnen The S-Unit. Hij stelt het team in staat om op een goede en fijne manier te werken en geeft naar eigen zeggen dan ook liever de briljante voorzet dan dat hij zelf het doelpunt maakt. Wat wil Ray nog graag bereiken met The S-Unit? Wat is het leukste dat hij bij The S-Unit heeft meegemaakt? En met welke collega zou Ray wel een week willen ruilen?

Wie ben je?
Ik ben Ray van Daalen, 55 jaar en ik woon sinds een jaar samen met Barbara in Harderwijk. We wonen daar erg fijn. Het is een toeristische stad aan het water, met veel historie, een oude stadskern, en er wordt veel georganiseerd waardoor er altijd een leuke sfeer is.

Ik ben ooit als infrastructuur specialist begonnen bij een groot ICT-consultancy bedrijf. Dat heb ik ongeveer 10 jaar gedaan, waarna ik in een management rol terecht ben gekomen, waarin ik aardig vergelijkbaar werk heb uitgevoerd als wat ik op dit moment doe bij The S-Unit. Zelf omschrijf ik het altijd als een “spin in het web” rol, waarbij ik verantwoordelijk ben voor de inhoud van de werkzaamheden, medewerkers en ook klantcontact heb. Juist die combinatie vind ik erg inspirerend, motiverend en bevredigend, omdat ik zowel van mensen, klanten als van inhoud houd. Dat heb ik lange tijd gedaan, maar op een bepaald moment vroeg Barry van Kampen, medeoprichter van The S-Unit, of ik bij The S-Unit wilde werken. Daar had ik wel oren naar. Op 1 oktober 2020, op mijn verjaardag nota bene, ben ik begonnen bij The S-Unit in de rol van Sales Manager. Ik kreeg toen de vraag of ik daar “ook even de planning bij wilde doen”. Dat “even” is inmiddels uitgegroeid tot een ontzettend belangrijke taak binnen The S-Unit, waarin heel veel verschillende dingen samenkomen. Toen Linda in dienst kwam, heeft zij de sales rol van mij overgenomen en ben ik mij volledig gaan richten op de operationele zaken.

Als je het hebt over operationele zaken, welke werkzaamheden vallen daaronder?
Dat gaat over de planning van onze medewerkers: dus waar zij aan werken en wanneer, zodat zowel zij als onze opdrachtgevers tevreden zijn. Daarnaast hou ik mij ook bezig met HR, het operationele reilen en zeilen op kantoor, maar ook bijvoorbeeld zaken als de leaseauto’s van onze medewerkers, de apparatuur die op kantoor en bij medewerkers thuis aanwezig is, urenverantwoording, en de administratie en facturatie. Dus dat is een heleboel.

Wat vind je het leukst aan je werk?
Het allerleukste aan mijn werk vind ik het om mensen beter te maken en te helpen ontwikkelen. Ik zorg er graag voor dat mensen nog beter, fijner, gemotiveerder en meer betrokken hun werk kunnen doen. Ik geef liever de briljante voorzet dan dat ik zelf het doelpunt maak. Dat was vroeger al zo toen ik nog voetbalde, en dat is eigenlijk nog steeds het geval. En in mijn functie kan ik dit goed tot uiting brengen.

Welke tips heb je voor iemand die dit werk wil doen?
Het is belangrijk dat je stevig in je schoenen staat. Daarnaast moet je zowel begrijpen wat er zich inhoudelijk binnen de organisatie afspeelt, als wat er onder de mensen leeft, welke wensen en behoeften zij hebben, en hoe je ervoor kan zorgen dat iedereen goed samenwerkt en we samen ons doel kunnen bereiken. Zeker in deze tijd is het belangrijk dat je als manager facilitair bent en er dus voor zorgt dat anderen fijn en goed kunnen werken, zodat je samen tot het beste resultaat komt.

Verder moet je het interessant en uitdagend vinden om je te begeven in de kern van het proces, waarbij misschien wel het belangrijkste is dat je snel kunt schakelen en dus flexibel bent. Ik stel mijn prioriteiten op basis van wat er in de organisatie gebeurt, en dus kan het altijd zo zijn dat er opeens iets gebeurt wat belangrijker is dan hetgeen ik op dat moment aan het doen ben. Dan moet je snel kunnen schakelen en niet in paniek raken. Los daarvan is een grote inzet ook onontbeerlijk, naast de nodigde efficiëntie en doelgerichtheid.

Wat wil je nog bereiken met The S-Unit?
Mijn grootste doel met The S-Unit is om een bedrijf te zijn dat niet te groot en niet te klein is, maar waar wij ons wel begeven in de top van de markt. Met een gemotiveerd, tevreden, trots en betrokken team wil ik hele leuke, kwalitatief hoogstaande en belangrijke en waardevolle dingen doen. Dat vind ik heel belangrijk voor zowel nu als in de toekomst, veel belangrijker dan veel geld verdienen. Geld verdienen komt vanzelf, maar is wel absoluut noodzakelijk om een organisatie goed te kunnen laten draaien, mensen juist te kunnen belonen en ontwikkelen, en te kunnen investeren in de toekomst met nieuwe diensten of middelen, maar dat is niet ons hoofddoel.

Wat is het leukste dat je bij The S-Unit hebt meegemaakt?
Dat is de mooie groei die wij als bedrijf hebben doorgemaakt de afgelopen jaren, met een geweldig team nu in een prachtig kantoor zitten, en dat we zo'n geweldig team hebben met zoveel talent en potentie. Om die groei van dichtbij mee te maken was en is heel mooi. Om daarnaast te horen dat medewerkers tevreden zijn, is helemaal geweldig.

De evenementen van The S-Unit wil ik ook graag vermelden. Bijvoorbeeld ons Security Update Event, waar we met velen samen zijn en een mooi evenement neerzetten voor onze klanten. Maar de eerste onlangs gehouden Team Dag vond ik ook erg leuk, dat er nog maar vele mogen komen.

Waar kunnen we je het hardst mee aan het lachen maken?
Dat vind ik een lastige vraag. De één lacht hard om Funniest Home Videos, de ander om een slapstick komedie. Ik kan om beide lachen, dat ligt er maar net aan waar het over gaat. Ik hou erg van een beetje cynische humor of als iemand even bij de neus wordt genomen. Zolang maar duidelijk is dat het op een leuke en grappige manier bedoeld is.

Wat heb je al jaren willen doen, maar is er nog niet van gekomen?
Barbara en ik hebben de laatste jaren ontdekt dat wij het erg leuk vinden om op vakantie te gaan en mooie reizen te maken. Dat kan een vakantie zijn naar een zonnig oord om lekker te relaxen, maar ook om met een auto door Toscane te crossen en mooie dingen te bezichtigen en de specifieke sfeer op te snuiven en van de natuur te genieten. Dat vinden we allebei erg leuk, maar daar hebben we in de praktijk vaak weinig tijd voor. Ik zou het leuk vinden om daar iets meer tijd voor te hebben. We houden allebei van de zon en lekker weer en daarom is een grote wens van mij om wellicht ooit te emigreren naar een zonnig warm land. Dat is niet iets wat ik nu zou willen doen, maar misschien voor in de toekomst.

> ***Ik geef liever de briljante voorzet dan dat ik zelf het doelpunt maak.***

Als je een week mocht ruilen met een collega; met wie zou dat zijn en waarom?
Ik ben jaren geleden bij The S-Unit begonnen als sales manager, dus ik weet hoe dat werk eruit ziet, daar zou ik om die reden niet mee willen ruilen. Zowel technisch werk als consultancy vind ik erg boeiend, beide heb ik in het verleden ook gedaan, maar als ik dan toch zou moeten kiezen zou ik wel eens willen ruilen met één van onze hackers. Ik vind hun werk erg fascinerend, buitengewoon knap en ik zou dat zelf ook wel willen meemaken om je ei erin kwijt te kunnen en "de boel stuk te maken".

Wil je nog een geheim met ons delen? Iets wat niemand van jou wist?
Het is misschien niet echt een geheim, maar ik kook altijd. Barbara doet het huishouden en ik kook. Barbara kan niet koken en dat moeten we ook niet willen haha, en zij stofzuigt liever dan dat ik dat doe. Ik kan ook prima de was draaien, ik woon ten slotte al meer dan 35 jaar op mezelf (met of zonder partner), maar daar mag ik niet aankomen. Ik laat dat graag zo. Verder zou ik het niet weten eerlijk gezegd.

The S-University

Bij The S-Unit streven wij er elke dag naar om de wereld een stukje veiliger te maken. Dat doen we met onze ethische hackers, consultants én samen met jou. Wij maken jou sterker door je kennis en vaardigheden te vergroten en je weerbaar te maken in de wereld van vandaag en morgen.

Met ons team van meer dan 20 experts in het internationale werkveld van cybersecurity horen en zien we dagelijks hoe de spreekwoordelijke brand kan ontstaan, hoe te blussen én hoe te voorkomen. Die kennis en kunde brengen we als onderdeel van onze missie – samen bouwen aan een veiligere digitale maatschappij – over op vakgenoten via onze S-University.

Vanuit het perspectief van een hacker geven wij jouw kennis en vaardigheden een boost. Hoe gaan hackers te werk? Wat zijn de potentiële gevolgen ervan? En het belangrijkste: hoe kun jij je hiertegen wapenen? Samen met jou kijken wij door de ogen van een hacker!

Van meer technische onderwerpen zoals hackpogingen op Mendix en Azure omgevingen en het ontwikkelen van webapplicaties conform de OWASP Top 10 tot organisatorische vraagstukken als het effectief opbouwen van security awareness, het inrichten van beveiligingsbeleid en -maatregelen (bijvoorbeeld conform ISO27000) en het reageren op incidenten en crisissituaties; The S-Unit is van alle offensieve markten thuis!

Omdat iedere organisatie uniek is, kunt u de specifieke invulling van wat we vanuit The S-University doen altijd op maat laten maken zodat het precies past bij specifieke behoeften en situaties.

Ons huidige trainingsaanbod

Ethical Hacking: Webapplicaties

Altijd al veiligere code willen schrijven? Leer dit aan de hand van de OWASP top 10. Niet alleen door het schrijven, maar ook door zelf te hacken!

Security in Microsoft 365 en Azure

Hoe veilig is jouw Azure omgeving? Wij leren je hoe Azure te hacken en hoe een omgeving veilig in te richten.

Mendix: hacken en beveiligen

Hoe kun je je Mendix applicatie hacken? Hoe kun je security meenemen in je Mendix applicatie? Leer de ins en outs en ga praktisch aan de slag.

Security Awareness

Hoe doen die hackers dat nou eigenlijk? Leer hoe hackers te werk gaan, en hoe jij je daar tegen kan beschermen!

Cybercrisis Simulatie

Leer hoe te handelen in een cybercrisis door de Tabletop training te volgen. Hierin wordt een realistische cyber crisissituatie gesimuleerd.

OSINT-workshop

Word Sherlock Holmes van het web. Leer technieken voor Open Source Informatievergaring en ontdek jouw digitale voetafdruk op het web.

Suggesties

Zou je graag een training willen volgen bij The S-Unit, maar bieden wij deze (nog) niet aan? Of heb je suggesties voor trainingen die voor meerdere organisaties relevant zijn? Ga naar *www.the-s-unit.nl/trainingen* en laat het weten. Wellicht vervult deze training binnenkort een vaste plek in het trainingsaanbod van The S-Unit!

Jong geleerd, veilig gedaan

Kinderen ontdekken steeds vroeger de digitale wereld. In deze tijd, waarin technologie een grote rol speelt, moeten kinderen zich bewust zijn van de risico's en hoe ze daarmee om kunnen gaan. Denk aan oplichting, fraude en gestolen wachtwoorden. Leeftijd maakt voor cybercriminelen geen verschil, maar juist de onwetendheid van deze jonge generatie zorgt voor deze kwetsbaarheid.

Net zoals we leren stoppen bij rood licht en doorrijden bij groen licht, moeten we kinderen leren hoe ze online moeten handelen. Wat mag wel en wat niet?

Bij The S-Unit streven we ernaar om de wereld veiliger te maken. We helpen organisaties om hun digitale weerbaarheid te verbeteren, maar we vinden het ook belangrijk dat kinderen zich bewust zijn van digitale gevaren en weten hoe ze ermee om moeten gaan. Daarom hebben we een educatief programma ontwikkeld voor basisschoolleerlingen (groep 5 tot en met 8). In deze lessen leren we kinderen op een interactieve en leuke manier essentiële kennis over cybersecurity en digitale veiligheid.

Een belangrijk onderdeel van deze lessen is HackShield, een innovatieve en speelse benadering van cybersecurity training. HackShield is een virtuele wereld waar kinderen als 'Cyber Agent' uitdagingen aangaan om de digitale wereld veilig te houden. Hier kunnen ze op een veilige manier praktijkervaring opdoen en leren over sterke wachtwoorden, phishing herkennen en persoonlijke gegevens beschermen. De lessen sluiten aan bij de belevingswereld van kinderen en maken complexe concepten begrijpelijk.

Door kinderen al vroeg bewust te maken van cybersecurity, leggen we een stevige basis voor veilig online gedrag. Omdat kinderen steeds jonger toegang hebben tot technologie, is het essentieel om ze de nodige tools en kennis te geven om zichzelf te beschermen. Door hen bewust te maken van online risico's en te leren hoe ze veilig kunnen navigeren, spelen we een cruciale rol in het versterken van digitale veiligheid, niet alleen voor organisaties, maar voor de hele toekomstige maatschappij.

GEZOCHT:

HACK SHIELD
FUTURE CYBER HEROES

SUPPORTERS DIE WILLEN BIJDRAGEN AAN EEN ONLINE VEILIGE GENERATIE

Over HackShield
HackShield maakt van kinderen tussen de 8 en 12 jaar oud Cyber Agents die zichzelf en hun omgeving kunnen beschermen tegen online gevaar. Via een spannend spel leren ze deze gevaren herkennen en voorkomen. Ze ontdekken wat de risico's van de online wereld zijn en kunnen hun (groot)ouders behoeden voor deze risico's. Zo blijven meerdere generaties online veilig!

HackShield is gratis beschikbaar als individuele game voor kinderen en als lespakket voor basisscholen.

Supporters
Supporters spelen een belangrijke rol binnen HackShield. Dankzij onze Supporters kunnen we HackShield doorontwikkelen en gratis blijven aanbieden aan alle kinderen en scholen in Nederland.

Daarom zijn wij altijd op zoek naar Supporters die HackShield financieel willen ondersteunen én als Leerkracht voor een Dag een gastles HackShield geven. Want als Supporter heb je het voorrecht om met de (aspirant) Cyber Agents aan de slag te gaan. Wie leert hier meer van, zij of jij?

Meer weten of supporter worden? Neem dan contact met ons op via: supporters@joinhackshield.com.

Samen strijden we voor dat ene doel: een online veilige generatie.

JoinHackShield.com

SECURITY UPDATE EVENT

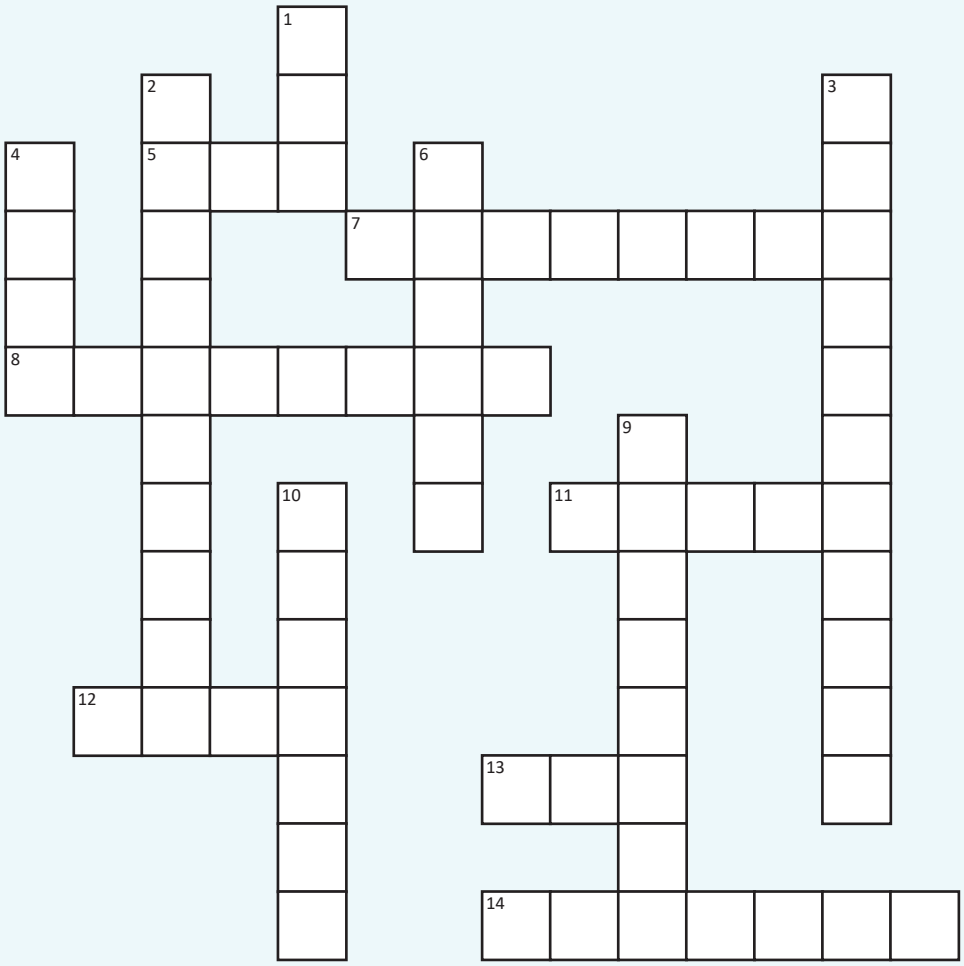
Op 31 maart vond het jaarlijkse Security Update Event plaats in het kantoor van The S-Unit. Met ruim 30 aanwezigen was het een zeer geslaagd evenement. Deelnemers werden bijgepraat over onder andere wachtwoordloos inloggen, Red Teaming en de nieuwe trainingen die The S-Unit aanbiedt (zie ook pagina 8 van dit e-magazine). Na de volledig verzorgde lunch gingen de aanwezigen tijdens de OSINT workshop op zoek naar wat er allemaal over hen te vinden is op het internet en sloten we het evenement af met een borrel.

SLOEPJE VAREN, ROSSEETJE DRINKEN

Op donderdag 6 juli was het weer tijd voor ons jaarlijkse team uitje! Met luxe motorsloepen ging het team van The S-Unit het water op voor een puzzeltocht op de Wijde Blik. En als dat nog niet genoeg was, genoten we daarna samen van een drankje en een uitgebreide barbecue. Lekker eten, drinken, en elkaar uitlachen als we geen idee hadden waar we naartoe voeren. Het was een gezellige en actieve middag!

THE S-UNIT CARIBBEAN

Het is ondertussen ruim twee jaar geleden dat onze collega Sara emigreerde naar het mooie Curaçao. Zoals Sara in een eerdere editie van dit e-magazine vertelde, was dit een droom die uitkwam. Zij maakte destijds bekend dat zij waarschijnlijk definitief op Curaçao wilde blijven wonen. Zo gezegd, zo gedaan: twee jaar later woont Sara niet alleen nog steeds op het prachtige Curaçao, ook The S-Unit heeft zich hier dit jaar definitief gevestigd. Begin maart zaten we bij de notaris op Curaçao en was The S-Unit Caribbean B.V. een feit!



Horizontaal

5 Een Europese verordening die de regels voor de verwerking van persoonsgegevens door bedrijven en overheidsinstanties in de EU standaardiseert.

7 Een computersysteem dat zich bewust kwetsbaar opstelt voor virussen en andere aanvallen.

8 Het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen.

11 Een schadelijk computerprogramma dat zich kopieert naar andere programma's en van binnenuit de computer kapotmaakt.

12 Een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken.

13 Een authenticatie methode waarbij de online gebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen.

14 Elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

Verticaal

1 Een fout in een computerprogramma of een website, waardoor het zijn functie niet (geheel) volgens specificaties vervult.

2 Malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'.

3 Een variant van phishing waarbij men via sociale netwerksites en datingsites probeert om persoonlijke gegevens te bemachtigen.

4 Een aanval waarbij er zoveel aanvragen naar de aangevallen website worden verzonden zodat deze de toestroom niet meer aankan en de website niet meer goed functioneert.

6 Een verzameling computers waarop malware is geïnstalleerd zonder dat de eigenaren zich daarvan bewust zijn.

9 Een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.

10 Een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt worden om in deze systemen in te breken.

OVER THE S-UNIT

Omdat IT van onschatbare waarde is om commerciële en maatschappelijke doelen te verwezenlijken zijn pogingen om onrechtmatige toegang tot uw informatie te krijgen helaas aan de orde van de dag. De ethical hackers van The S-Unit onderwerpen organisaties daarom aan gesimuleerde cyberaanvallen zodat kwetsbaarheden onder veilige omstandigheden aan het licht komen. Naast de op maat gemaakte pentensten, heeft The S-Unit specialisten huis die kunnen helpen bij Red Teaming opdrachten, Consultancy en het inwinnen van kennis en kunde omtrent security. Binnen onze Academy geven wij bijvoorbeeld workshops, organiseren we CTF events en hebben we The S-University voor trainingen. Bezoek onze website voor het gehele aanbod van onze services.

Meer weten over The S-Unit of de diensten die wij aanbieden? Bezoek onze website of neem contact met ons op!

Savannahweg 71
3542 AW Utrecht

030 207 4177

info@the-s-unit.nl

THE S-UNIT FLYERS

Wil je meer weten over The S-Unit en/of de diensten die wij aanbieden? Download gratis onze flyers over onder andere The S-Unit, pentesting, red teaming, CTF-games, security awareness, cybercrisis simulatie, CLaaS en Kraken! Download de flyers hier:

DOWNLOAD

THE S-UNIVERSITY

De website van The S-Unit is aangevuld met alle trainingsdata voor 2024! Dus: ben je op zoek naar een boost voor je cybersecurityvaardigheden? Of wil je aan de slag met het verhogen van cyberveiligheid van jouw organisatie? Bekijk nu alle trainingen op onze website: *www.the-s-unit.nl/trainingen*

Bij The S-Unit kun je daarnaast deze hele week nog profiteren van onze Cyber Monday-actie*: 20% korting op al onze trainingen. Kortom, registreer je nu en gebruik de code *CYBERMONDAY-TSU*

**Deze kortingscode is geldig t/m 3 december 2023*